An introduction to the Sweden Connect Technical Framework

2024-12-04

Reference number: **2019-267**

Table of contents

1. Introduction

1.1. Overview

The Sweden Connect Technical Framework is adapted for identity federations based on SAML 2.0.

> In the latest version of the Technical Framework, specifications for OpenID Connect have also been introduced. Currently, there is no federation support for OpenID Connect. This will be introduced in 2025.
>
> The remaining parts of this document only describe the SAML federation. Once OpenID Connect has been fully introduced, this document will also cover this technology.

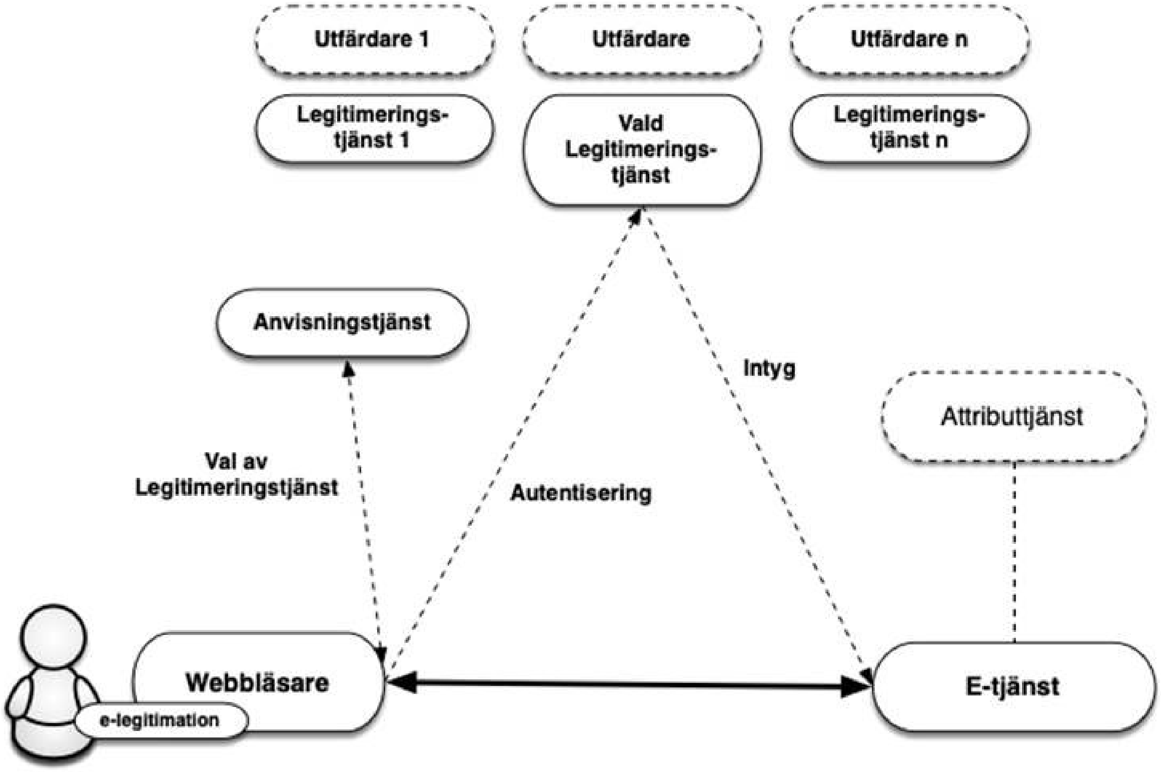
Relying parties receive identity certificates in a standardised format from an authentication service[1].

E-services that require a signature do not need to be adapted to different users' eIDs in order to create electronic signatures. Instead, the e-service delegates this to a signature service, where users, supported by authentication through an authentication service, are given the opportunity to sign electronic documents.

Within the federation, e-services and corresponding relying parties assume the role of Service Provider (SP), while authentication services issuing identity certificates assume the role of Identity Provider (IdP) and thus the authenticator of the user, regardless of the e-service for which the user being authenticated.

For those cases where the e-service needs more information about the user, e.g. information about legal capacity, a question can be asked to an attribute service, Attribute Authority (AA), within the federation, if such a relevant attribute service exists. Through an attribute request, the e-service can obtain the necessary additional information to authorise the user and provide access to the e-service or equivalent.

As both personal identity data and other attributes associated with users are provided through identity certificates and attribute certificates, all types of eIDs that relying parties have an agreement on and that are part of the federation can be used for authentication vis-á-vis an e-service that requires both a personal identity number and additional information, even if the eID does not contain any specific personal data (e.g. code boxes for the generation of one-time passwords).



Utfärdare 1	Issuer 1
Utfärdare n	Issuer n

Legitimeringstjänst 1	Authentication service 1
Vald legitimeringstjänst	Selected authentication service
Legitimeringstjänst n	Authentication service n
Anvisningstjänst	Discovery service
Intyg	Certificate
Val av legitimeringstjänst	Choice of authentication service
autentisering	authentication
attributtjänst	attribute service
Webbläsare	Browser
E-tjänst	E-service

Figure 1: *Illustration of the communication between the different services within an identity federation.*

[1]: The authentication service is also referred to in other documentation from Digg as an identity service and a certification service. In this document, however, only the term ‘authentication service’ is used.

1.2. Trust framework and security levels

The basis for which security level is to applied when a user is being authenticated is the assurance level for the e-identification required by the e-service. In order for these security levels to be comparable within the framework of the federation, four assurance levels (1-4) are defined in the Trust Framework for Swedish e-identification [Digg.Tillit] and three assurance levels (low, substantial, high) in the EU’s eIDAS Regulation. All identity certificate issuers must demonstrate that the entire process underpinning the issuance of identity certificates meets the requirements of the required assurance level, including:

- requirements for the creation of the identity certificate;
- requirements for electronic identification (authentication);
- requirements for the issuing process;
- requirements for the eID itself and its use;
- requirements for the eID issuer;
- requirement for establishing the identity of the eID applicant.

1.3. Service for the collection, administration and publication of metadata

An SAML federation provides information about the federation’s participants through SAML metadata. Both entities that provide authentication and attribute services in the federation as well as relying parties, i.e. entities that consume these services, e.g. e-services, are considered to be participants in a federation.

The federation’s metadata allows participants to obtain information on the services of other participants, including the data necessary for the secure exchange of information between participants. Metadata must be kept up to date by each party and in accordance with contractual conditions.

The main purpose of metadata is to provide the keys/certificates required for secure communication and information exchange between services. In addition to keys, metadata also contains other information that is important for the interaction between services, such as addresses of required functions, information about assurance levels, service categories, user interface information, etc.

An identity federation is defined by a registry in XML format that is signed with the federation operator's certificate. The file contains information about the members of the identity federation, including their certificates. Since the metadata file is signed, it is sufficient to compare a certificate with its metadata counterpart. An infrastructure based on a central federation registry requires that the registry be continuously updated and that the federation members always use the latest version of the file.

1.4. Discovery service

In an identity federation, it is possible to offer and consume a shared discovery service, which lists the authentication services available for the user to choose from. The purpose of such a discovery service is to relieve the individual e-services that are part of the identity federation from implementing support with respect to how users choose the authentication service (or login method).

Since the discovery service is available within the identity federation, e-services can direct their users there in order to choose the authentication service. The discovery service interacts with the user who makes their choice, and the user, together with the user's choice, is directed back to the e-service, which now knows to which authentication service the user should be sent for authentication.

> There is currently no shared discovery service for the Sweden Connect federation.

1.5. Integration at the relying party

Relying parties, e.g. e-services, integrate with authentication services through standardised messages and consume identity certificates which also have standardised formats.

The Sweden Connect technical framework is influenced by the interoperability profile 'SAML V2.0 Deployment Profile for Federation Interoperability' [SAML2Int]. The profile is supported by a number of commercial products and Open Source solutions, which facilitates integration at e-services.

Many e-services use stand-alone authentication solutions, which means that adapting the integration to comply with the technical framework has a limited impact on the e-service as such.

1.6. Signature

When signing, the Sweden Connect technical framework makes it possible to use different types of eID, even those that are not certificate-based, without the need for special adaptations in the e-service. This is because the electronically issued identity certificate (used for identification of users when signing) has the same format regardless of the type of eID used by the user.

A signature service aims to enable signatures within identity federations that comply with the technical framework, supported by all types of eID that offer a sufficient degree of security.

By procuring[1] and introducing a signature service, a relying party that is part of the federation can allow a user to sign an electronic document with the support of the signature service. The user's electronic signature and associated signing certificate are created by the signature service after the user has agreed to sign by authenticating themselves vis-á-vis the signature service[2].

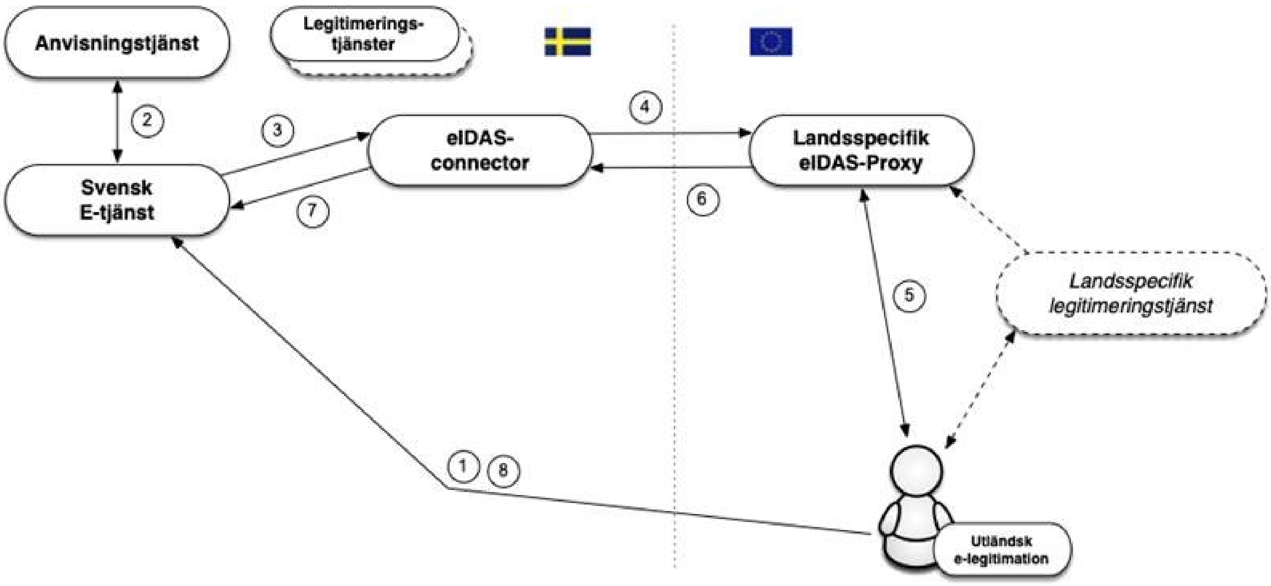
> [1]: It is also possible to implement a signature service based on the specifications of the technical framework, or otherwise acquire a signature service.
>
> [2]: It is important to note that it is of the utmost importance that the user perceives this process as signing a document. Therefore, a signature flow should be used for the eIDs that support this in connection with 'authentication for signature'.

1.7. Technical framework and eIDAS

The EU Regulation (910/2014) on electronic identification and trust services, eIDAS, requires Swedish public bodies to recognise the eIDs that other eIDAS countries have notified. This means that a public Swedish e-service based on certain rules must be able to accept a login performed using an eID issued in another country.

1.7.1. Authentication using foreign eIDs

The technical specifications for eIDAS are based, like the technical framework, on SAML standards, and although there are many similarities, there are also differences in these specifications. However, a Swedish e-service should not relate directly to the technical specifications of eIDAS. The image below illustrates how the Swedish eIDAS node (*eIDAS-connector*) acts as a bridge between other countries and the Swedish federation when a person is being authenticated using a foreign eID in a Swedish e-service. The Swedish eIDAS node complies with the technical framework.



Anvisningstjänst	Discovery service
Legitimeringstjänster	Authentication services
Svensk E-tjänst	Swedish e-service
EiDAS-connector	eiDAS-connector
Landsspecifik Eidas Proxy	Country-specific eIDAS proxy
Landsspecifik legitimeringstjänst	Country-specific authentication service
utländsk e-legitimation	foreign eID

The flow is as follows:

1. A user with a foreign eID requests access to a Swedish e-service (i.e. logs in).

2. The e-service allows the user to choose the login method using a discovery service. A ‘Foreign eID’ option is displayed, which is selected by the user in the eIDAS case.

3. The e-service creates an authentication request in accordance with this technical framework and directs the user to the Swedish eIDAS node (*connector*) for which DIGG is responsible. The eIDAS node acts as an authentication service (*Identity Provider*) in the federation vis-á-vis Swedish relying parties, which means that communication with this service is carried out in the same way as with other authentication services within federations that comply with technical framework.

4. The received request is processed and the eIDAS node displays a selection page where the user selects ‘their country’[1]. The Swedish eIDAS node now converts the received authentication request into an eIDAS authentication request and directs the user to the selected country’s ‘eIDAS proxy service’.

5. When the authentication request is received by the eIDAS proxy service for the selected country, this country’s authentication technology takes over. Not all eIDAS countries use SAML for authentication, but if this were the case in our example, the

user would be redirected to an authentication service (*Identity Provider*), and before that perhaps also a discovery service for the selection of the authentication service.

6. Once authentication has been performed, a certificate (*Assertion*) is created according to eIDAS specifications. This certificate includes eIDAS-specific attributes that identify the user. This certificate is now forwarded to the Swedish eIDAS node.

7. The node receives the certificate and validates its accuracy. This certificate is transformed from eIDAS format into a certificate formatted according to the technical framework and is mailed to the e-service.

8. The relying party adds any additional information and determines whether the user should be granted access to the service.

Swedish e-services thus only need to support the technical framework in order to handle an authentication performed using a European eID. However, the e-service must be able to handle the identity presented, which is not necessarily a personal identity number. Thus, there may be instances where an e-service authenticates a user via the eIDAS framework, but the user’s presented identity cannot be used in the e-service. More on this in Chapter 1.7.3 below.

[1]: Actually, the user chooses the ‘eIDAS proxy service’ to which the request should be forwarded. This is dependent on the country to which the user’s eID issuer belongs.

1.7.2. Signatures using foreign eIDs

As already described, a model for electronic signature is applied within this technical framework called federated signature. A server-based signature service is linked to the e-service, which in turn requests a signature. When a user signs a document, the e-service sends a signature request to the signature service. The signature service then requests the user to authenticate themselves. In connection with the authentication, the user approves the signature. The signature service sends data back to the e-service, and then the signature data associated with the document that has been signed is stored.

This procedure makes it possible to sign also using a foreign eID, as the signature service can choose to authenticate the user using a foreign eID in accordance with the procedure described above in section 1.7.1.

When signing, in this case, the Swedish eIDAS node is responsible for informing the user that the purpose of the authentication is to sign a document, who requested the signature, and any information about what is being signed. An identity certificate is only issued once the user has authenticated themselves (for signature) and this is sent to the signature service and which in turn generates the signature.

1.7.3. Management of identities

Identity certificates from other countries comply with EU-wide technical specifications developed within the framework of the eIDAS Regulation. The attributes that each country must always include for natural persons as well as for organisations (‘Minimum Dataset’, MDS) are laid down in this Regulation. Each country must include a unique identifier per eID representing only one natural person. From some countries, these identifiers will be unique and persistent per person in the same way as, for example, Swedish personal identity numbers, but these identifiers can have very different compositions and characteristics. One characteristic that can vary is how persistent such an identifier is, i.e. whether such an identifier remains unchanged during a person's lifetime or changes if, for example, the person moves to another region, changes their name, or just changes their eID. From some countries (e.g. the UK), the identifier will vary depending on which of the country's eIDs a user currently chooses to use.

In order to simplify the management of users in Swedish e-services, the Swedish eIDAS node generates a standardised ID attribute for users who have been authenticated using foreign eID, known as a *provisional ID* (abbreviated as PRID). In addition, an associated attribute is created that declares the expected persistence, or lifespan, of this ID attribute. The PRID attribute is generated based on the attribute values obtained from the foreign authentication according to specified methods for that particular country. Each combination of country and method is categorised in terms of expected persistence, i.e. how likely it is that an identity changes over time for the same person. This enables Swedish e-services to adapt communication with the user and proactively provide features that make it easier for a user whose identity has changed to regain control over their information in the e-service.

In some cases, a person who is authenticated using a foreign eID may also hold a Swedish personal identity number. This may, for example, be a Swedish citizen who has moved abroad and obtained a foreign eID or a foreign citizen who is registered in Sweden and has been assigned a personal identity number.

The fact that a person with a foreign eID has a Swedish personal identity number is not normally known to the foreign authentication service, and this information is therefore not included in the identity certificate from the country where the person is authenticated. The Swedish node, on the other hand, has the ability to query an attribute service in Sweden[1] as to whether there is a registered personal identity number for the authenticated person and can, if this is the case, add such information to the identity certificate sent to the e-service.

[1]: At the time of writing, there is no attribute service that establishes a link between eIDAS identities and Swedish personal identity numbers.

1.7.4. Swedish eIDs in foreign e-services

Sweden has notified Swedish eIDs at the assurance levels substantial and high according to eIDAS.

A request for authentication from a foreign e-service is made to the Swedish eIDAS node (proxy service) via an eIDAS connector in the country of the e-service. In the Swedish eIDAS node, the user chooses which Swedish eID they wish to use to authenticate with, and then an authentication request is sent to the authentication service (*Identity Provider*) that handles the selected eID. This request is formatted according to a technical framework, which means that a Swedish authentication service does not have to comply with eIDAS technical specifications.

The user is authenticated by the Swedish authentication service and an identity certificate is issued (according to the technical framework). This certificate is received by the Swedish eIDAS proxy service and converted into a certificate according to eIDAS specifications before it is forwarded to the foreign eIDAS connector and then to the calling e-service (*Service Provider*).

2. Technical specifications

This chapter contains specifications and profiles for identity federations that comply with the Sweden Connect technical framework, and certain related services. Unless otherwise stated, these documents are prescriptive for the delivery of services within identity federations that implement the technical framework.

2.1. Profiles and specifications for SAML

Identity federations that comply with the Sweden Connect technical framework are built around the ‘Deployment Profile for the Swedish eID Framework’, [SAML.Profile]. This profile is influenced by, but not prescriptively dependent on, the ‘SAML V2.0 Deployment Profile for Federation Interoperability’ [SAML2Int]. [SAML.Profile] also contains rules and guidelines specific to the Sweden Connect technical framework.

2.1.1. Deployment Profile for the Swedish eID Framework

‘Deployment Profile for the Swedish eID Framework’, [SAML.Profile], is the main technical framework document and specifies, inter alia:

- how SAML metadata shall be constructed and interpreted;
- how the authentication request shall be formatted;
- how an authentication request shall be handled, and how an identity certificate shall be designed, verified and handled;
- security requirements;
- specific SAML requirements for signature services and ‘authentication for signature’.

2.1.2. Swedish eID Framework – Registry for identifiers

Implementation of a Swedish eID infrastructure requires different forms of identifiers to represent objects in data structures. The document ‘Sweden Connect – Registry for identifiers’, [SC.Registry], defines the structure of identifiers assigned under the technical framework, as well as a register of defined identifiers.

2.1.3. Attribute Specification for the Swedish eID Framework

The specification ‘Attribute Specification for the Swedish eID Framework’, [SAML.Attributes], declares the SAML attribute profiles that are used within identity federations that comply with the technical framework including those that connect to eIDAS via the Swedish eIDAS node.

2.1.4. Entity Categories for the Swedish eID Framework

Entity Categories are used within the federation for a number of different purposes:

- Service Entity Categories – Used in metadata to represent e-services' requirements for assurance levels and requested attributes, as well as authentication services' fulfilment of assurance levels and delivery of attributes.
- Service Property Categories – Used to represent a specific characteristic of a service.
- Service Type Entity Categories – Used to represent different service types within the federation.
- Service Contract Entity Categories – Used by services to announce agreement forms and the like.
- General Entity Categories – Entity Categories that do not fall within any of the above types.

The specification 'Entity Categories for the Swedish eID Framework' [SAML.EntCat] specifies the entity categories defined by the technical framework and describes their meaning.

2.1.5. eIDAS Constructed Attributes Specification for the Swedish eID Framework

The specification 'eIDAS Constructed Attributes Specification for the Swedish eID Framework', [SC.eIDAS.Attrs], specifies processes and rules for how ID-attributes are constructed based on attributes received duringauthentication in eIDAS.

2.1.6. Implementation Profile for BankID Identity Providers within the Swedish eID Framework

The specification 'Implementation Profile for BankID Identity Providers within the Swedish eID Framework', [SAML.BankID], defines rules for how an authentication service that implements support for BankID shall be designed.

> **Please note the following:** This specification is not prescriptive for compliance with a technical framework. It is only relevant for authentication services that implement support for BankID and e-services that use these. However, authentication services that implement support for BankID and want to connect to the Sweden Connect federation must comply with this specification.

2.1.7. Principal Selection in SAML Authentication Requests

The specification 'Principal Selection in SAML Authentication Requests', [SAML.Principal], defines an extension to SAML that enables a relying party to inform an authentication service which identity it wishes to be authenticated.

2.1.8. User Message Extension in SAML Authentication Requests

The specification 'User Message Extension in SAML Authentication Requests', [SAML.UMessage], defines an extension to SAML that enables a relying party to include a display message in the authentication request sent to the authentication service. The authentication service can then show this message to the user during the authentication step.

2.2. Profiles and specifications for OpenID Connect

2.2.1. OpenID Connect Profile for Sweden Connect

The profile ‘OpenID Connect Profile for Sweden Connect’, [OIDC.Profile], builds on the Swedish OpenID Connect Profile which is an OpenID Connect profile developed by OIDC Sweden to promote interoperability and security within Swedish OIDC solutions.

[OIDC.Profile] adds additional requirements concerning the Sweden Connect federation.

2.2.2. OpenID Connect Claims and Scopes Specification for Sweden Connect

The specification ‘OpenID Connect Claims and Scopes Specification for Sweden Connect’, [OIDC.Claims], builds on the specification Claims and Scopes Specification for the Swedish OpenID Connect Profile from OIDC Sweden.

2.3. Specifications for Signature

This section contains references to the documents defining signature services within federations that comply with the Sweden Connect technical framework.

2.3.1. Implementation Profile for using OASIS DSS in Central Signing Services

The implementation profile ‘Implementation Profile for Using OASIS DSS in Central Signing Services’, [Sign.DSS.Profile], specifies a profile for the signature request and response according to the OASIS standard ‘Digital Signature Service Core Protocols, Elements, and Bindings’, [DSS].

2.3.2. DSS Extension for Federated Central Signing Services

‘DSS Extension for Federated Central Signing Services’, [Sign.DSS.Ext], is an extension of the OASIS standard ‘Digital Signature Service Core Protocols, Elements, and Bindings’, [DSS], which specifies definitions necessary for signing under the technical framework.

2.3.3. Certificate Profile for Certificates Issued by Central Signing Services

The certificate profile ‘Certificate profile for certificates issued by Central Signing services’, [Sign.Cert.Profile], specifies the content of signing certificates. This profile applies a new certificate extension to support signature services.

This profile refers to the ‘Authentication Context Certificate Extension’, [AuthContext], which describes how the ‘Authentication Context’ is represented in X.509 certificates.

2.3.4. Signature Activation Protocol for Federated Signing

The specification ‘Signature Activation Protocol for Federated Signing’, [Sign.Activation], defines a ‘Signature Activation Protocol’ (SAP) for the implementation of ‘Sole Control Assurance Level 2’ (SCAL2) according to the standard ‘prEN 419241 – Trustworthy Systems Supporting Server Signing’.

3. Reference list

3.1. DIGG

[Digg.Tillit]

Trust framework for Swedish e-identification.

[SC.Registry]

Sweden Connect – Registry for identifiers.

[SAML.Profile]

Deployment Profile for the Swedish eID Framework.

[SAML.Attributes]

Attribute Specification for the Swedish eID Framework.

[SAML.EntCat]

Entity Categories for the Swedish eID Framework.

[SC.eIDAS.Attrs]

eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[SAML.BankID]

Implementation Profile for BankID Identity Providers within the Swedish eID Framework.

[SAML.Principal]

Principal Selection in SAML Authentication Requests.

[SAML.UMessage]

User Message Extension in SAML Authentication Requests.

[OIDC.Profile]

OpenID Connect Profile for Sweden Connect.

[OIDC.Claims]

OpenID Connect Claims and Scopes Specification for Sweden Connect.

[Sign.DSS.Profile]

Implementation Profile for Using OASIS DSS in Central Signing Services.

[Sign.DSS.Ext]

DSS Extension for Federated Central Signing Services.

[Sign.Cert.Profile]

Certificate profile for certificates issued by Central Signing services.

[Sign.Activation]

Signature Activation Protocol for Federated Signing.

3.2. Other references

[SAML2Int]

SAML V2.0 Deployment Profile for Federation Interoperability.

[DSS]

OASIS Standard – Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, April 11, 2007.

[AuthContext]

RFC-7773: Authentication Context Certificate Extension.